BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	WO 98/26554
H04L 29/06, 12/56, 29/12	A1	(43) International Publication Date:	18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/22540

(22) International Filing Date: 8 December 1997 (08.12.97)

(30) Priority Data:
08/762,709 9 December 1996 (09.12.96) US

(71) Applicants: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Avenue, Mail Stop PAL1-521, Palo Alto, CA 94303 (US). MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: WONG, Thomas, K.; 1118 Matara Court, Pleasanton, CA 94566 (US). LIM, Swee, B.; 11691 Timber Spring Court, Cupertino, CA 95014 (US). RADIA, Sanjay, R.; 883 Boar Circle, Fremont, CA 94539 (US). TSIRIGOTIS, Panagiotis; 801 W. El Camino Real #142, Mountain View, CA 94040 (US). GOEDMAN, Robert, J.; 755 Holly Oak Drive, Palo Alto, CA 94303 (US). PATRICK, Michael, W.; 9 Elizabeth Drive, Assonet, MA 02702 (US).

(74) Agents: MAJERUS, Laura, A. et al.; Graham & James LLP, 600 Hansen Way, Palo Alto, CA 94304 (US).

(81) Designated States: JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR ASSIGNMENT OF IP ADDRESSES

(57) Abstract

A preferred embodiment of the present invention includes a method and apparatus for allocating and using IP addresses in a network of client systems. More specifically, the present invention includes a router which monitors the assignments of IP adresses by a DHCP server. As each IP address is assigned, the router associates the assigned IP address with a trusted identifier which identifies the client system. Subsequently, if the router receives a packet directed at the assigned IP address, the router forwards the packet to the client system having a trusted identifier associated with the destination address of the IP packet. Additionally, if the router receives a packet from a client system, it uses the trusted identifier of the client system to find IP addresses associated with the client system. If the source address of the IP packet is not included in the IP addresses associated with the client system, the packet is discarded.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method and Apparatus for Assignment of IP Addresses

FIELD OF THE INVENTION

The present invention relates generally to security in computer networks. More specifically, the present invention is a method and apparatus for assignment of IP addresses that discourages IP address forging.

BACKGROUND OF THE INVENTION

Recent years have witnessed an explosive growth in the use of computer networks. In fact, the use of computer networks to connect disparate computer systems around the world has become a routine and accepted fact. One result of the ever-increasing use of computer networks is an ever-increasing need for security systems.

Computer networks that use the Internet protocol are commonly referred to as "IP networks." Within IP networks, host systems and other objects are identified by thirty-two bit numbers, known as Internet Protocol Addresses (IP addresses). IP addresses provide a simple mechanism for identifying the source and destination of messages sent within IP networks. Unfortunately, several methods exist that allow IP addresses to be falsified, or forged. By forging an IP address, a malicious user may usurp messages within the IP network, possibly gaining access to sensitive information. Forging IP address also allows malicious users to send bogus messages. These messages can easily have a negative impact on network security if a receiving system accepts them as genuine. In a general sense, the possibility that IP addresses may be forged forces systems within IP networks to assume that IP addresses are unreliable.

The unreliability of IP addresses has also discouraged the development and use of programs known as "packet filters." More specifically, packet filters are programs that are positioned at key points within an IP network, such as within network routers. Packet filters examine packets that cross these key points and discard those packets that appear to present a threat to network security.

An example of packet filtering would be a company that uses a router to link its internal intranet with an external network, such as the Internet. In such a

network, a packet filter positioned within the router could inspect the header of each received packet to determine the address of the system sending the packet. Clearly, in this case, packets that arrive from the Internet but that have source addresses that correspond to addresses of systems within the company intranet are suspect. A packet filter included in a router would, therefore, discard packets of this type.

The preceding example of a packet filter works well because it assumes that the source address included in a IP packet may be forged. In fact, the example packet filter is designed to detect this type of forged source address. Unfortunately, the unreliability of IP addresses has, to some extent, discouraged a more generalized use of packet filtering systems.

SUMMARY OF THE INVENTION

A preferred embodiment of the present invention includes a method and apparatus for assignment of IP addresses that discourages IP address forging. More specifically, a preferred environment for the present invention is a computer network that includes a series of client systems. Each client system is connected to a corresponding cable modem that is connected, in turn, to a router. An access network control server (ANCS) controls configuration of the router. A services management system (SMS) dynamically reconfigures the ANCS. The network includes one or more DHCP server systems that provide for allocation of IP addresses in accordance with the Dynamic Host Configuration Protocol (DHCP) defined in Internet RFC 1541.

On power-on, each client system requests an IP address by broadcasting a DHCPDISCOVER message to the network using one of the cable modems. The router receives the DHCPDISCOVER message and forwards the DHCPDISCOVER message to the DHCP servers within the network. Before forwarding the DHCPDISCOVER message, however, the router encodes a trusted identifier into the vendor-specific options field of the DHCPDISCOVER message. The trusted identifier is an unforgeable object that positively identifies the client system sending the DHCPDISCOVER message. For a preferred

embodiment of the present invention, the trusted identifier is the id of the cable modem from which the DHCPDISCOVER message was received.

In response to the DHCPDISCOVER message, a DHCPACK message is generated by one of the DHCP servers. The DHCPACK message includes an IP address for the client system and the trusted identifier originally encoded in the DHCPDISCOVER message by the router. The router listens for DHCPACK messages and when, one is received, examines the included IP address and trusted identifier. Using the trusted identifier and the IP address included in the DHCPACK message, the router "learns" the address of each client system requesting an IP address. In this way, the router forms an association between the IP address and the trusted identifier. An IP address associated with a trusted identifier is called a "learned" IP address.

When the router receives a packet directed at a learned IP address, it forwards the packet to the modem that is associated with the learned IP address. This action prevents client systems from usurping IP addresses to gain illicit access to IP packets. Additionally, when the router receives a packet from a modem, it compares the source address included in the packet with the IP addresses that are associated with that modem. If the packet does not originate from an IP address that the router recognizes as being associated with the sending modem, the packet is discarded.

In accordance with the purpose of the invention, as embodied and broadly described herein, the present invention is a method for allocating and using IP addresses in a computer network that includes one or more client systems connected to a router, each client system having an associated trusted identifier, with the router system being able to send IP packets to an individual client system using the trusted identifier associated with the client system, the method comprising the steps, performed by the router, of: detecting a request made by a client system for allocation of an IP address, encoding the trusted identifier associated with the client system in the request, detecting a response to the request from a DHCP server, the response including an IP address allocated to the client system, the response including a copy of the trusted identifier encoded

in the request, associating the IP address included in the response with the client system trusted identifier included in the response, and forwarding the response to the client system using the trusted identifier included in the response.

In further accordance with the purpose of the invention, as embodied and broadly described herein, the present invention is a computer program product comprising: a computer usable medium having computer readable code embodied therein for allocating and using IP addresses in a computer network that includes one or more client systems, each client system having an associated trusted identifier, the computer program product comprising: first computer readable program code devices configured to cause a computer system to detect a request made by a client system for allocation of an IP address, second computer readable program code devices configured to cause the computer system to encode the trusted identifier associated with the trusted identifier in the request, and third computer readable program code devices configured to cause the computer system to detect a response to the request from a DHCP server, the response including an IP address allocated to the client system, the response including a copy of the trusted identifier encoded in the request, fourth computer readable program code devices configured to cause the computer system to associate the IP address included in the response with the client system trusted identifier included in the response, and fifth computer readable program code devices configured to cause the computer system to forward the response to the client system using the trusted identifier included in the response.

Advantages of the invention will be set forth, in part, in the description that follows and, in part, will be understood by those skilled in the art from the description or may be learned by practice of the invention. The advantages of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims and equivalents.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and, together with the description, serve to explain the principles of the invention.

Figure 1 is a block diagram of a computer network shown as a representative environment for a preferred embodiment of the present invention.

Figure 2 is a block diagram of a router used by a preferred embodiment of the present invention.

Figure 3 is a block diagram of an access network control server (ANCS) as used by a preferred embodiment of the present invention.

Figure 4 is a block diagram of an services management system (SMS) as used by a preferred embodiment of the present invention.

Figure 5 is a block diagram of a DHCP message used in a preferred embodiment of the present invention.

Figure 6 is a flowchart showing the steps associated with a preferred embodiment of the IP address learning method of the present invention.

Figure 7 is a flowchart showing the steps, performed by the router, for a preferred embodiment of the IP address learning method of Figure 6.

Figure 8 is a flowchart showing the steps, performed by the router, for a preferred embodiment of the packet forwarding method of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

In Figure 1, a computer network 100 is shown as a representative environment for the present invention. Structurally, computer network 100 includes a series of client systems 102, of which client systems 102a through 102f are representative. Each client system 102 may be selected from a range of differing devices including, but not limited to, the personal computers shown in Figure 1. A cable modem 104 is connected to each client system 102. Each cable modem 104 is connected, in turn, to a cable router 106. The use of cable router

106 and cable modems 104 is also intended to be exemplary and it should be appreciated that other networking technologies and topologies are equally practical. It should also be appreciated that a number of different cable modems and cable routers are available from various manufactures. In particular, cable modem 104 can be a CyberSUFR cable modem and cable router 106 can be a CableMASTR cable router, both supplied by Motorola, Inc.

Router 106 is shown in more detail in Figure 2 to include a computer system 202 that, in turn, includes a processor, or processors 204, and a memory 206. An input device 208 and an output device 210 are connected to the computer system 202 and represent a wide range of varying I/O devices such as disk drives, keyboards, modems, network adapters, printers and displays. A disk drive 212, of any suitable disk drive type, is shown connected to computer system 202. A router management process 214 is shown to be resident in memory 206 of computer system 202.

Computer network 100 also includes a series of server systems 108, of which server systems 108a through 108c are representative. Each server system 108 is connected to cable router 106. Generally, server systems 108 are intended to represent the broad range of server systems that may be found within computer networks.

Computer network 100 also includes an access network control server (ANCS) 110 and a services management system (SMS) 112. Both ANCS 110 and SMS 112 are connected to cable router 106. ANCS 110 is shown in more detail in Figure 3 to include a computer system 302 that, in turn, includes a processor, or processors 304, and a memory 306. An input device 308 and an output device 310 are connected to the computer system 302 and represent a wide range of varying I/O devices such as disk drives, keyboards, modems, network adapters, printers and displays. A disk drive 312, of any suitable disk drive type, is shown connected to computer system 302. An ANCS process 314 is shown to be resident in memory 306 of computer system 302.

SMS 112 is shown in more detail in Figure 4 to include a computer system 402 that, in turn, includes a processor, or processors 404, and a memory 406. An

input device 408 and an output device 410 are connected to the computer system 402 and represent a wide range of varying I/O devices such as disk drives, keyboards, modems, network adapters, printers and displays. A disk drive 412, of any suitable disk drive type, is shown connected to computer system 402. A SMS filter management process 414 and filtering profile database 416 are shown to be resident in memory 406 of computer system 402.

A DHCP server system 114 is also included in computer network 100 and connected to cable router 106. DHCP server system 114 is a computer or other system that implements Dynamic Host Configuration Protocol (DHCP) defined in Internet RFC 1541, which is incorporated herein by reference. Functionally, DHCP server system 114 provides for allocation of IP addresses within network 100. Although Figure 1 shows only a single DHCP server system 114, it is to be understood that additional DHCP server systems 114 may be used without departing from the spirit of the present invention. It should also be appreciated that the connections between the various components of Figure 1 are intended to represent logical connections. The actual physical topology used for these connections may vary from what is pictured in Figure 1.

A preferred format for DCHP messages sent between client systems 102 and DHCP server system 114 is shown in Figure 5 and generally designated 500. Structurally, a DCHP message includes an op field 502, a yiaddr field 504, a chadddr field 506 and an options field 508 (Examination of Figure 5 shows that each message also includes a number of other fields. For the sake of brevity, these fields will not be discussed with particularity). Functionally, each DHCP message has a type, such as DHCPDISCOVER, DHCPOFFER, DHCPREQUEST or DHCPACK. The type of each DHCP message is encoded into the options field 508. The options field is also used for a number of other purposes, including the encoding of vendor-specific information. Each DHCP message is marked to indicate whether it is being sent from a client system 102 or a DHCP server system 114. This marking is performed by setting op 502 to BOOTREQUEST, or BOOTREPLY, respectively. Within a message, the yiaddr field 504 includes, for certain types of DHCP messages 500, an IP address being passed from a DHCP

server 114 to a client system 102. The chadddr field 506 is used for the machine address of a client system 102 (also known as a "MAC" address).

In a preferred embodiment of the present invention, router 106 learns IP addresses assigned by DHCP server system 114. A preferred embodiment of this method is shown in Figure 6 and generally designated 600. Method 600 includes steps performed by a client system 102, steps performed by router 106 and steps performed by DHCP server 114. For convenience, these steps are shown to be included in a client system context 602, a router context 604 and a DHCP server context 606, respectively.

Method 600 begins, in client context 602, with step 608. Step 608 is initiated when a client system 102 powers on or otherwise initially connects to cable router 106. As part of this power-on sequence, the client requests an IP address by broadcasting a DCHPDISCOVER message through cable modem 104 to router 106. Preferably, the DCHPDISCOVER message is constructed in accordance with message format 500 with op 502 set to BOOTREQUEST, chaddr field 506 set to the machine address of the client system 102 and DCHPDISCOVER encoded in options field 508. In step 608, this DCHPDISCOVER message is sent by client system 102 through modem 104 to router 106 for broadcast to all DHCP server systems 114.

In step 610, the DCHPDISCOVER message is received by the router 106. The router 106 recognizes that the received message is a DCHPDISCOVER message. Accordingly, the router 106 encodes a trusted identifier into the vendor-specific information included in the options field 508 of the DCHPDISCOVER message. The trusted identifier is an unforgeable object that positively identifies the client system 102 sending the DHCPDISCOVER message. For a preferred embodiment of the present invention, the trusted identifier is the id of the cable modem 104 from which the DHCPDISCOVER message was received. The id of the cable modem 104 is received by the router 106 when the modem was initialized via message(s) passed between the modem and the router at that time. In step 612, the router 106 broadcasts the DCHPDISCOVER message, now including the trusted identifier, to all DHCP server systems 114.

In step 614, the DCHPDISCOVER message is received from the router 106 by DHCP server system 114. Subsequently, in step 616, the DHCP server system 114 responds to the DCHPDISCOVER message by formulating a DHCPOFFER message. The DHCPOFFER message is preferably constructed using format 500 with op 502 set to BOOTREPLY and DHCPOFFER encoded in the options field 508. The chaddr field 506 and vendor-specific information included in the options field 508 of the DHCPOFFER message are copied from the DCHPDISCOVER message. As a result, the trusted identifier is now included in the DHCPOFFER message. Additionally, the yiaddr field 504 is set to an IP address that the DHCP server 114 has allocated for the use of the client system 102. In step 616, this DHCPOFFER message is sent by the DHCP server 114 to the router 106

In step 618, the router 106 receives the DHCPOFFER message and forwards the message to the modem 104 for receipt by client system 102. Importantly, the message is forwarded exclusively to the modem identified by the trusted identifier embedded in the vendor-specific options field of the DHCPOFFER message.

In step 620, the DHCPOFFER message is received by the client system 102. The client system 102 may accept the DHCPOFFER message or wait for DHCPOFFER messages from other DHCP servers 114. For the purposes of illustration, however, it is assumed in Figure 6 that the client system 102 accepts the first DHCPOFFER message received. The client system 102 responds to the DHCPOFFER message by constructing and sending a DHCPREQUEST message to the DHCP server 114. The DHCPOFFER message is constructed using format 500 with op 502 set to BOOTREQUEST and DHCPREQUEST encoded in the options field 508. The chaddr field 506 and vendor-specific information included in the options field 508 of the DHCPREQUEST message are copied from the DHCPOFFER message. As a result, the trusted identifier is now included in the DHCPREQUEST message. In step 622, this DHCPREQUEST message is sent by the client system 102 to the router 106.

In step 624, the router 106 receives the DHCPREQUEST message and forwards the message to the DHCP server 114. In step 626, the DHCP server system 114 receives the DHCPREQUEST message. Subsequently, in step 628, the DHCP server system 114 responds to the DHCPREQUEST message by formulating a DHCPACK message. The DHCPACK message is preferably constructed using format 500 with op 502 set to BOOTREPLY and DHCPACK encoded in the options field 508. The chaddr field 506 and vendor-specific information included in the options field 508 of the DHCPACK message are copied from the DHCPREQUEST message. As a result, the trusted identifier is now included in the DHCPACK message. Additionally, the yiaddr field 504 is, once again, set to the IP address that the DHCP server 114 has allocated for the use of the client system 102. In step 628, the DHCP server 114 sends the DHCPACK message to the router 106.

In step 630, the router 106 receives the DHCPACK message. The router 106 recognizes that the received message is a DHCPACK message. Accordingly, the router 106 extracts the trusted identifier from the vendor-specific information included in the options field 508 of the DHCPACK message. The router 106 also extracts the IP address allocated by the DHCP server 114 from the yiaddr field 504 of the DHCPACK message. The router 106 then forms an association between the extracted trusted identifier and the extracted IP address. This association may be maintained in a list or other suitable data structure within memory 206 of computer system 202. Preferably, the association formed between the extracted trusted identifier and the extracted IP address is two-way. Using the two-way association the router 106 can determine the IP addresses that are associated with a modem 104. The router 106 can also determine which modem 104 is associated with an IP address. Effectively, by forming this association, the router 106 has learned the IP address allocated by the DHCP server 114. In step 632, the router 106 forwards the DHCPACK message to the modem 104 for receipt by client system 102. Importantly, the message is forwarded exclusively to the modem identified by the trusted identifier embedded in the vendor-specific options field of the DHCPACK message.

In step 634, the client system 102 receives the DHCPACK message. The client system 102 then uses the IP addresses included in the yiaddr field 504 of the DHCPACK message as the IP address of the client system 102.

For clarity, the steps performed by the router 106 for a preferred embodiment of the IP address learning method are shown as method 700 of Figure 7. More specifically, method 700 begins with step 702 where the router 106 receives a message. In step 704 the received message is examined, by the router 106, to determine if the message is a DHCPDISCOVER message. In the affirmative case, execution of method 700 continues at step 706 where the router 106 encodes the trusted identifier of the client system 102 sending the DHCPDISCOVER message into the vendor-specific information included in the options field 508 of the DHCPDISCOVER message. The router 106 then forwards the DHCPDISCOVER message in step 708.

In the alternative case to step 704, (i.e., where the received message is not a DHCPDISCOVER message) execution of method 700 continues at step 710. In step 710, the received message is examined to determine if it is a DHCPACK message. In the affirmative case, execution of method 700 continues at step 712 where the router 106 checks to see if the IP address allocated by the DHCP server has been previously associated with another trusted identifier.

In the positive case (i.e., where the IP address has been previously associated with another trusted identifier) execution of method continues at step 714. In step 714 the router 106 removes the association between the allocated IP address and the other trusted identifier. This prevents a single IP address from being associated with multiple trusted identifiers. Execution of method 700 then continues at step 718 where the router 106 associates the IP address included in the yiaddr field 504 of the DHCPACK message with the trusted identifier included in the vendor-specific information included in the options field 508 of the DHCPACK message. As discussed previously, this association may be performed using any suitable data structure that allows for a two-way association between trusted identifier and IP addresses.

A preferred embodiment of the present invention also includes a method using for selectively forwarding, by router 106, of packets based on learned assignments of IP addresses. A preferred embodiment of this method is shown in Figure 8 and generally designated 800. Method 800 begins with step 802 where an IP packet is received by the router 106. In step 804 that follows, the received IP packet is examined to determined if it is a "downstream packet." Generally, routers categorize packets into "upstream" and "downstream" packets. In the case of the network topology shown for network 100, upstream packets are packets that originate at one of the client systems 102. Downstream packets are packets that are directed at one of the client systems 102.

If a downstream packet is detected in step 804, execution of method 800 continues at step 806 where the router 106 extracts the packet's destination address. Using this destination address, the router 106, in step 808 "looks up" the trusted identifier of the client system 102 that is associated with the destination address of the received packet (this association is formed by the router 106 during execution of method 600). In step 810, a test is performed to ascertain whether a trusted identifier was actually located in step 808. If a trusted identifier was located in step 808, execution of method 800 continues at step 812 where the router 106 forwards the received packet to client system associated with the trusted identifier. In the alternative, if no trusted identifier is associated with the destination address of the packet, the router 106 discards the packet in step 814.

If a downstream packet is not detected in step 804 (i.e., when the packet is an upstream packet), execution of method 800 continues at step 816, where the router 106 extracts the packet's source address. In step 818, the router 106 retrieves the trusted identifier of the client system 102 from which the IP packet was received. In step 820, the router 106 "looks up" the IP addresses that are associated with the trusted identifier retrieved in the previous step. For the purposes of the present invention, these IP addresses are the only IP addresses that are authorized to send packets using the modem 104 from which the packet was received.

In step 822, the router 106 compares the source address of the received packet with the authorized IP addresses that were looked up in step 820. If the source address of the packet matches one of the authorized IP addresses, the router 106 forwards the packet in step 824. Alternatively, if the source address of the received packet does not match one of the authorized IP addresses, the router 106 discards the packet in step 826.

It should be appreciated that the use in the preceding description of the use of cable modems 104 and a cable router 106 with regard to Figures 1 through 8 is intended to exemplary. In particular, it should be appreciated that the present invention is specifically intended to be used in combination with a wide range of networking technologies and topologies. The present invention is particularly applicable to networks, like network 100, that provide for an id that is associated with each client system 102 and that allow packets to be sent exclusively to a particular client system 102 using the id of the client system 102.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope of the invention being indicated by the following claims and equivalents.

WHAT IS CLAIMED IS:

1. A method for allocating and using IP addresses in a computer network that includes one or more client systems connected to a router, each client system having an associated trusted identifier, with the router system being able to send IP packets to an individual client system using the trusted identifier associated with the client system, the method comprising the steps, performed by the router, of:

detecting a request made by a client system for allocation of an IP address;

encoding the trusted identifier associated with the client system in the request;

detecting a response to the request from a DHCP server, the response including an IP address allocated to the client system, the response including a copy of the trusted identifier encoded in the request;

associating the IP address included in the response with the client system trusted identifier included in the response; and

forwarding the response to the client system using the trusted identifier included in the response.

2. A method as recited in claim 1 further comprising the steps, performed by the router, of:

receiving an IP packet sent by one of the client systems;

using the trusted identifier of the sending client system to retrieve IP addresses associated with the sending client system;

retrieving a source IP address from the IP packet; and

conditionally discarding the IP packet if the source IP address is not included in the IP addresses associated with the sending client system.

3. A method as recited in claim 1 further comprising the steps, performed by the router, of:

receiving an IP packet being sent to one of the client systems;

retrieving a destination IP address from the IP packet;

using the destination IP address to retrieve the trusted identifier of the client system associated with the destination IP address; and

forwarding the IP packet to the client system using the retrieved trusted identifier.

4. A method as recited in claim 1 wherein the detected request made by a client system for allocation of an IP address is a DHCPDISCOVER message.

5. A method as recited in claim 4 wherein the step of encoding the trusted identifier associated with the client system, is performed by encoding the trusted identifier in the vendor-specific information of the DHCPDISCOVER message.

6. A method as recited in claim 1 wherein the detected response to the request from a DHCP server is a DHCPACK message.

7. A method as recited in claim 1 wherein the router included in the computer network is a cable router and wherein the network includes one or more cable modems with each client system being connected to the to the cable router using one such cable modem and wherein the trusted identifier associated with each client is the modem id of the cable modem to which the client system is connected.

8. A computer program product comprising:

a computer usable medium having computer readable code embodied therein for allocating and using IP addresses in a computer network that includes one or more client systems, each client system having an associated trusted identifier, the computer program product comprising:

first computer readable program code devices configured to cause a computer system to detect a request made by a client system for allocation of an IP address;

second computer readable program code devices configured to cause the computer system to encode the trusted identifier associated with the trusted identifier in the request; and

third computer readable program code devices configured to cause the computer system to detect a response to the request from a DHCP server, the response including an IP address allocated to the client system, the response including a copy of the trusted identifier encoded in the request;

fourth computer readable program code devices configured to cause the computer system to associate the IP address included in the response with the client system trusted identifier included in the response; and

fifth computer readable program code devices configured to cause the computer system to forward the response to the client system using the trusted identifier included in the response.

9. A computer program product as recited in claim 8 which further comprises:

sixth computer readable program code devices configured to cause the computer system to receive IP packets sent by the client systems, each IP packet including a source IP address;

seventh computer readable program code devices configured to cause the computer system to use the trusted identifier of each client system sending IP packets to retrieve IP addresses associated with each client system sending IP packets; and

eighth computer readable program code devices configured to cause the computer system to conditionally discard an IP packet if the source IP address included in the IP packet is not included in the IP addresses associated with the client system sending the IP packet.

10. A computer program product as recited in claim 8 which further comprises:

sixth computer readable program code devices configured to cause the computer system to receive IP packets sent to one of the client systems, each IP packet including a destination IP address;

seventh computer readable program code devices configured to cause the computer system to use the destination IP address of each received IP packet to retrieve the trusted identifier of the client system associated with the destination IP address; and

eighth computer readable program code devices configured to cause the computer system to forward the received IP packet to the client system associated with the destination IP address.

11. A computer program product as recited in claim 8 wherein the detected request made by a client system for allocation of an IP address is a DHCPDISCOVER message.

12. A computer program product as recited in claim 12 wherein the trusted identifier associated with the client system is encoded in the vendor-specific information of the DHCPDISCOVER message.

13. A computer program product as recited in claim 8 wherein the detected response to the request from a DHCP server is a DHCPACK message.

14. An apparatus for allocating and using IP addresses in a computer network that includes one or more client systems connected to a router, each client system having an associated trusted identifier, with the router system being able to send IP packets to an individual client system using the trusted identifier associated with the client system, the method comprising the steps, performed by the router, of:

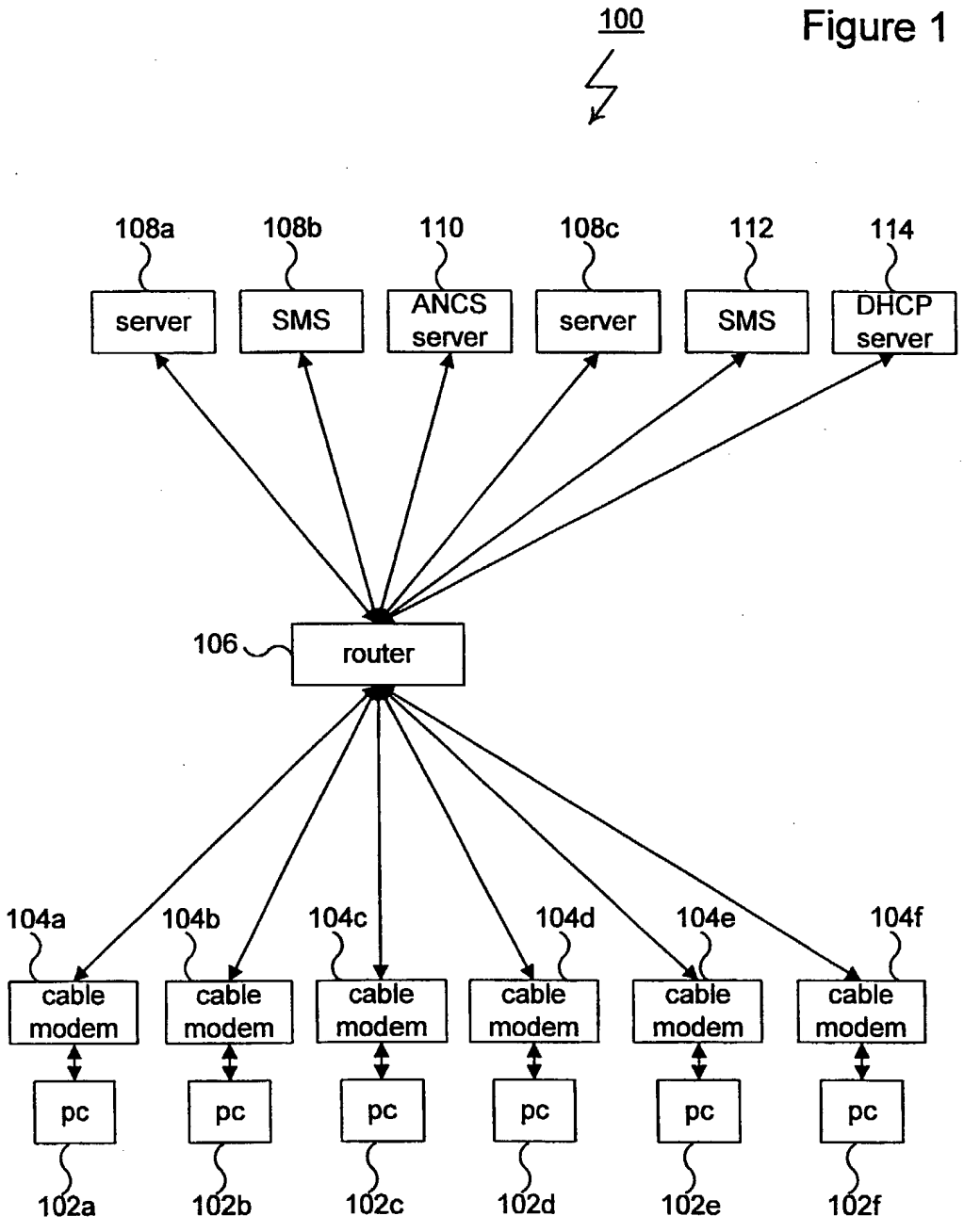
a first portion configured to cause the router to detect the assignment of an IP addresses to a client system and to associated the IP address assigned to a client system with the trusted identifier of the client system;

a second portion configured to cause the router to accept an IP packet directed at a client system, the accepted IP packet including a destination IP address, the second portion also configured to cause the router to use the

destination IP address of the accepted IP packet to retrieve the trusted identifier of the client system associated with the destination IP address and to forward the accepted IP packet to the client system associated with the destination IP address; and

a third portion configured to cause the router to accept an IP packet sent from a client system, the accepted IP packet including a source IP address, the third portion also configured to cause the router to use the trusted identifier of the sending client system to retrieve IP addresses associated with the sending client system and to conditionally discard the accepted IP packet if the source IP address included in the accepted IP packet is not included in the IP addresses associated with the sending client system.

Figure 1


100
108a
server
108b
SMS
110
ANCS server
108c
server
112
SMS
114
DHCP server
106
router
104a
cable modem
104b
cable modem
104c
cable modem
104d
cable modem
104e
cable modem
104f
cable modem
pc
pc
pc
pc
pc
pc
102a
102b
102c
102d
102e
102f

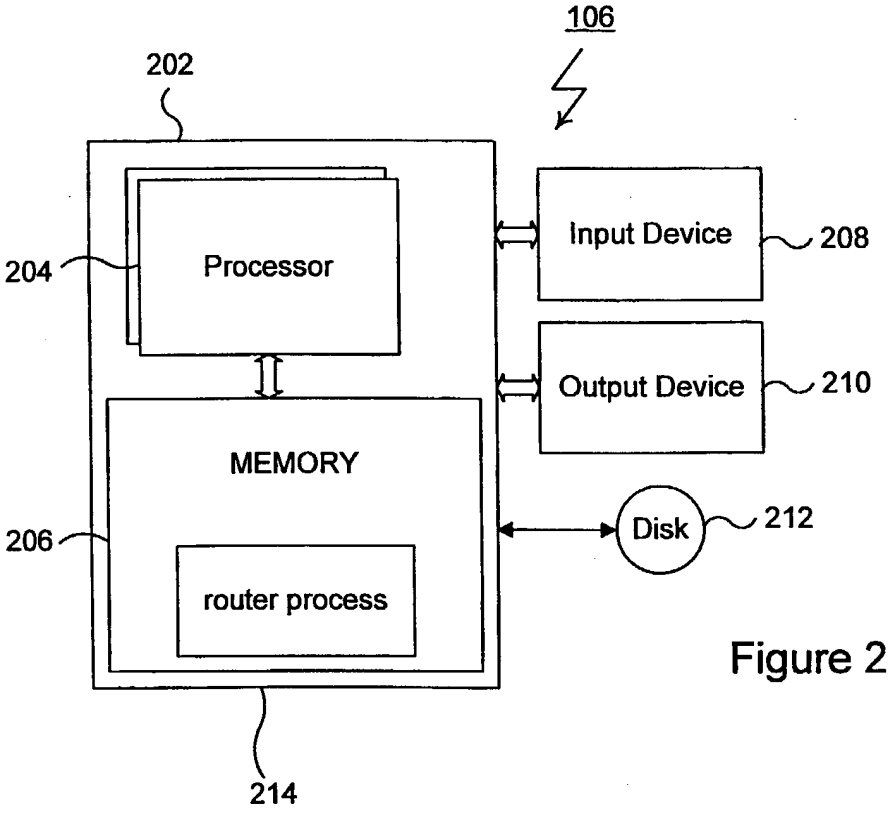


Figure 2

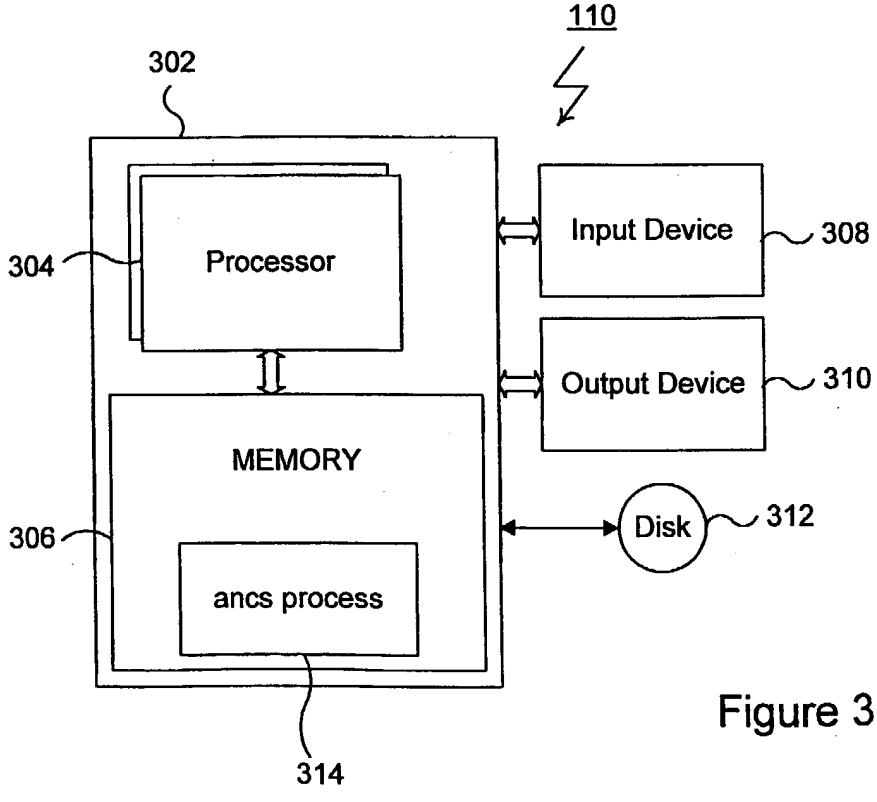
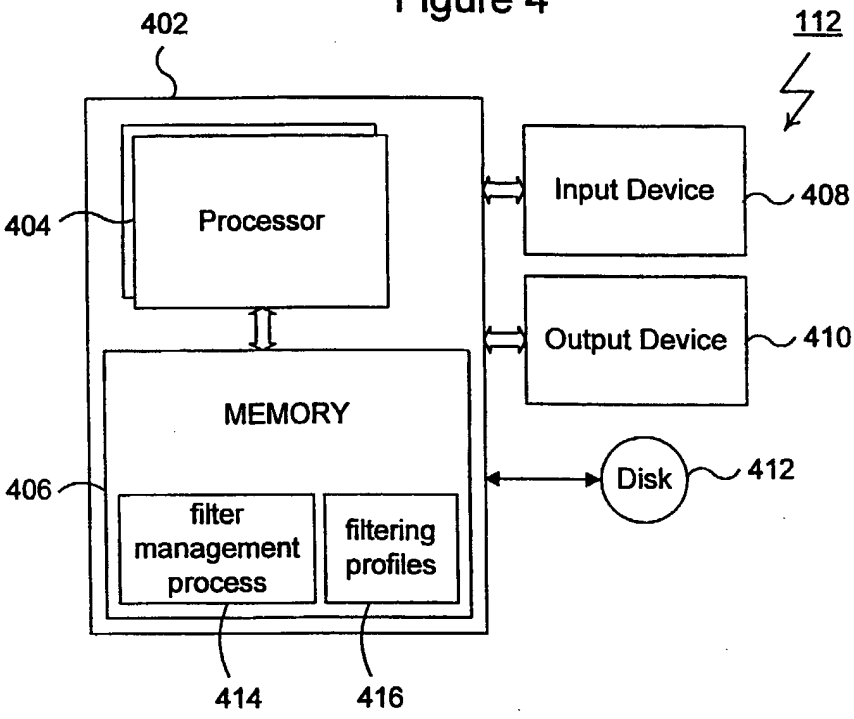


Figure 3

Figure 4



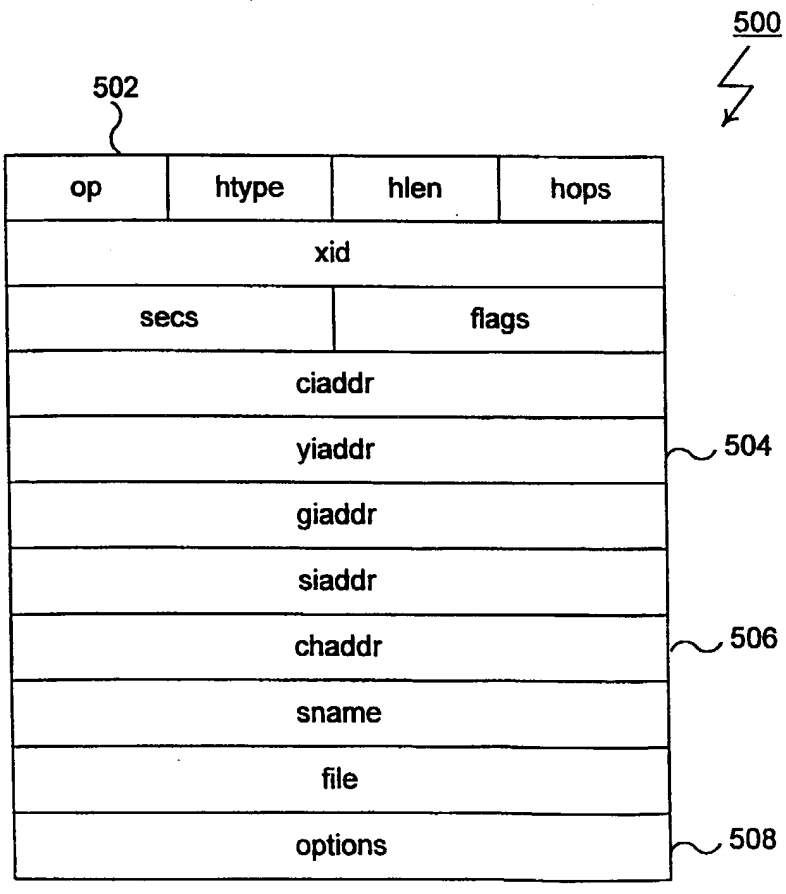


Figure 5

Figure 6

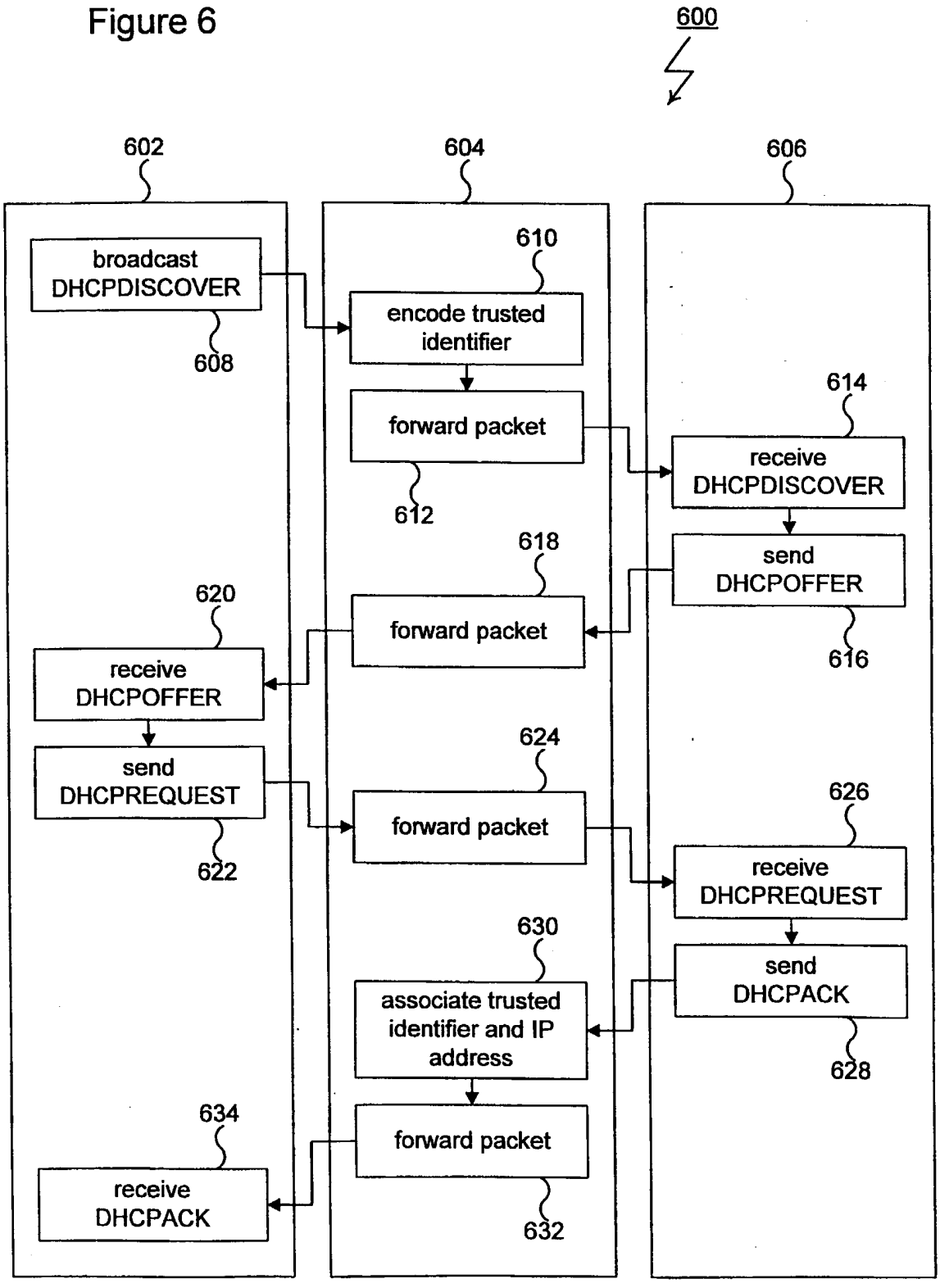

600
602
604
606
broadcast DHCPDISCOVER
608
610
encode trusted identifier
forward packet
612
614
receive DHCPDISCOVER
send DHCPOFFER
616
618
forward packet
620
receive DHCPOFFER
send DHCPREQUEST
622
624
forward packet
626
receive DHCPREQUEST
send DHCPACK
628
630
associate trusted identifier and IP address
forward packet
632
634
receive DHCPACK

Figure 7

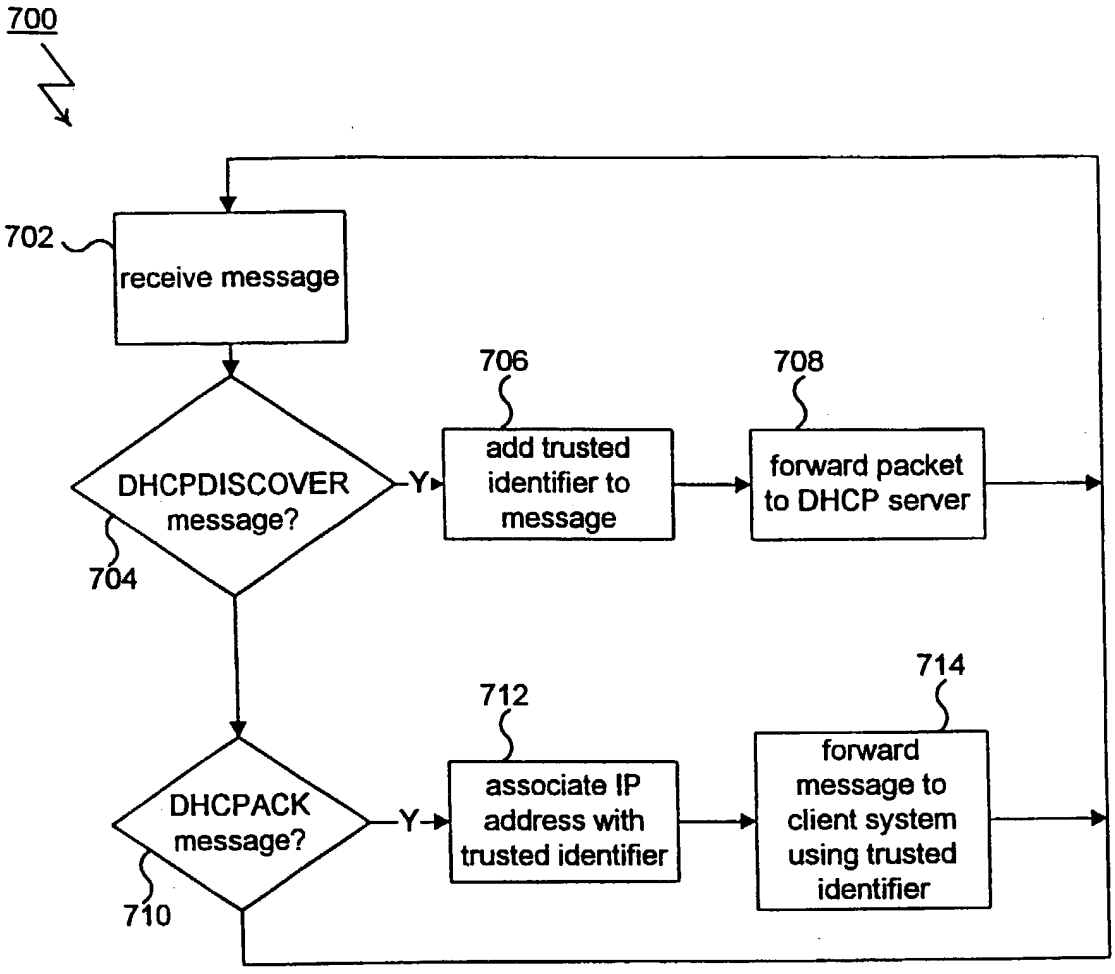
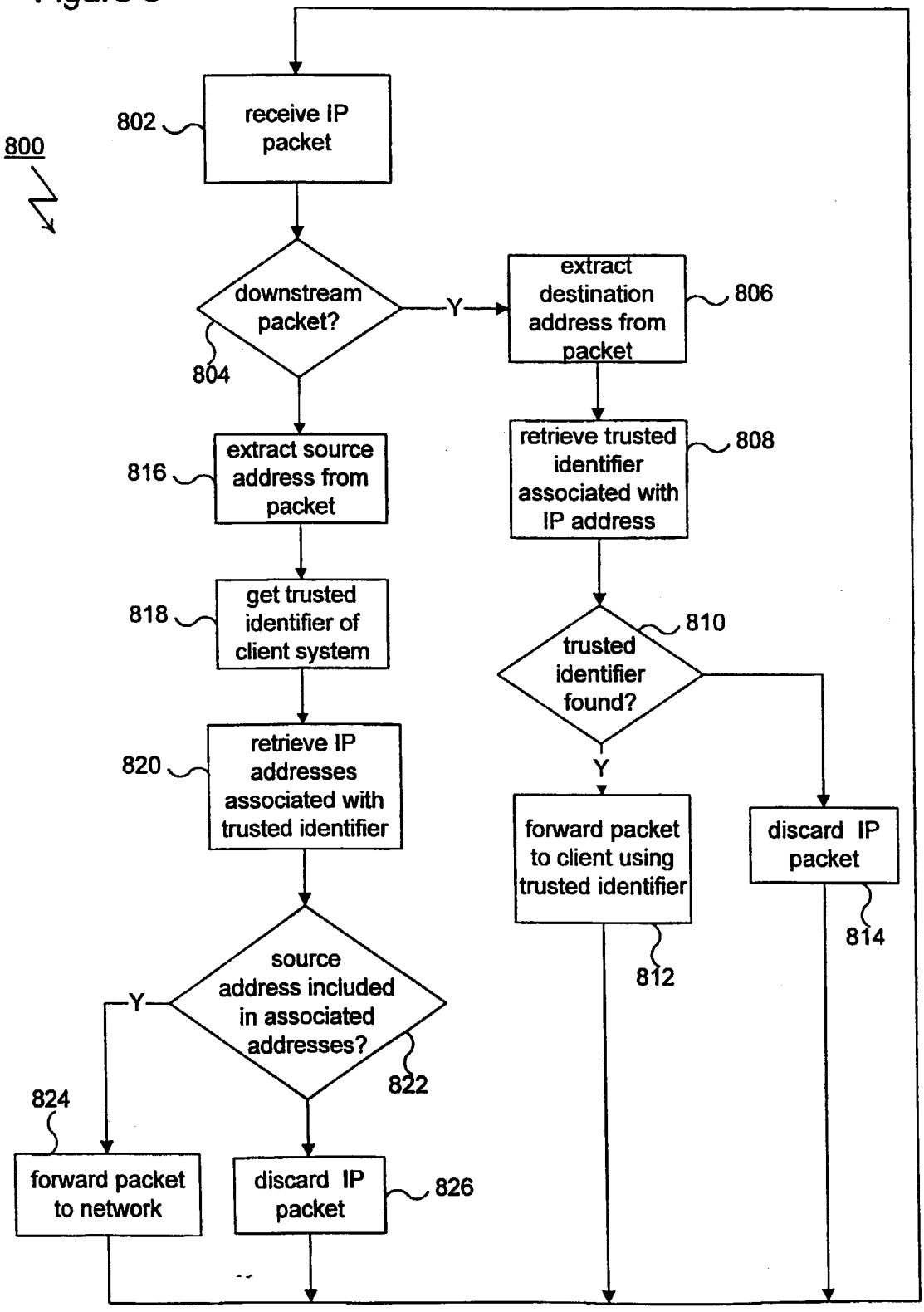

700
702
receive message
DHCPDISCOVER message?
Y
704
706
add trusted identifier to message
708
forward packet to DHCP server
DHCPACK message?
Y
710
712
associate IP address with trusted identifier
714
forward message to client system using trusted identifier

Figure 8


800
802
receive IP packet
downstream packet?
804
Y
extract destination address from packet
806
retrieve trusted identifier associated with IP address
808
trusted identifier found?
810
Y
forward packet to client using trusted identifier
812
discard IP packet
814
extract source address from packet
816
get trusted identifier of client system
818
retrieve IP addresses associated with trusted identifier
820
source address included in associated addresses?
822
Y
824
forward packet to network
discard IP packet
826

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 97/22540

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 H04L12/56 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PERKINS C E ET AL: "USING DHCP WITH COMPUTERS THAT MOVE" WIRELESS NETWORKS, vol. 1, no. 3, 1 October 1995, pages 341-353, XP000538245 see page 342, left-hand column, line 52 - right-hand column, line 13 see page 342, right-hand column, line 24-27 see page 343, left-hand column, line 28-36 see page 352, left-hand column, line 31-51 see figure 2 --- -/--	1,8,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

4

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 1998	14/05/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. ...nal Application No
PCT/US 97/22540

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DOUGLAS E. COMER: "Internetworking with TCP/IP. Volume 1: Principles, Protocols, and Architecture." 1995 , PRENTICE HALL INTERNATIONAL EDITIONS , NEW JERSEY XP002063312 see paragraph 21.9 - paragraph 21.18 ---	3-7, 11-13
P,X	WO 96 39769 A (SHIVA CORP) 12 December 1996	1,8,10
A	see abstract see page 2, line 8-28 see page 3, line 6-19 see page 4, line 1-23 ---	2,9,14
A	PATENT ABSTRACTS OF JAPAN vol. 096, no. 011, 29 November 1996 & JP 08 186569 A (TOSHIBA CORP), 16 July 1996, see abstract ---	1,2,8,9, 14
A	EP 0 483 547 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 6 May 1992 see abstract see column 3, line 20-34 see column 5, line 29-47 see column 5, line 57 - column 6, line 2 see column 6, line 51 - column 7, line 7 -----	1,2, 8-10,14

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/US 97/22540

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9639769 A	12-12-96	AU 5441696 A	24-12-96
		EP 0830772 A	25-03-98
EP 483547 A	06-05-92	US 5159592 A	27-10-92
		DE 69119353 D	13-06-96
		DE 69119353 T	07-11-96
		JP 2516291 B	24-07-96
		JP 4227149 A	17-08-92